Fields of Parametrization and Optimal Affine Reparametrization of Rational Curves

Luis Felipe Tabera[*]

October 30, 2008

Abstract

In this paper we present three related results on the subject of fields of parametrization. Let $\mathcal{C}$ be a rational curve over a field of characteristic zero. Let $\mathbb{K}$ be a field finitely generated over $\mathbb{Q}$, such that it is a field of definition of $\mathcal{C}$ but not a field of parametrization. It is known that there are quadratic extensions of $\mathbb{K}$ that parametrize $\mathcal{C}$. First, we prove that there are infinitely many quadratic extensions of $\mathbb{K}$ that are fields of parametrization of $\mathcal{C}$.

As a consequence, we prove that the witness variety, that appear in the context of the parametric Weil's descente method, is always a special curve related to algebraic extensions, called hypercircle. It is possible that the witness variety is not a hypercircle for the given extension, but for an alternative one.

We use these two facts to present an algorithm to solve the following optimal reparametrization problem. Given a birational parametrization $\phi(t)$ of a curve $\mathcal{C}$, compute the affine reparametrization $t \to at + b$ such $\phi(at + b)$ has coefficients over a field as small as possible. The main advantage of this algorithm is that it does not need to compute any rational point on the curve.

1   Introduction

Let $\mathbb{K}$ be a characteristic zero field, $\mathbb{F}$ its algebraic closure. Let $\mathcal{C} \subseteq \mathbb{F}^N$ be a rational curve. We say that $\mathbb{K}$ is a *field of definition* of $\mathcal{C}$ if $\mathcal{C}$ can be described as the zero set of a system of polynomials with coefficients in $\mathbb{K}$. Analogously, we say that $\mathcal{C}$ is *parametrizable* over $\mathbb{K}$ if there is a parametrization of $\mathcal{C}$ defined by rational functions in $\mathbb{K}(t)$. Given any rational curve $\mathcal{C}$ there is a well defined notion of field of definition k of $\mathcal{C}$ which is the smallest field of definition under inclusion. However, if $\mathcal{C}$ is not parametrizable over its smallest field of definition, the best we can say is that there are minimal fields of parametrization that are quadratic algebraic extensions of k [4, 12, 6].

In this article we study how many minimal fields of parametrization $\mathcal{C}$ has. The answer is trivial if $\mathcal{C}$ is parametrizable over its smallest field of definition, but it is more subtle if $\mathcal{C}$ is not parametrizable over k. We prove, using elementary tools from commutative algebra, that there are infinitely many quadratic algebraic extensions $k(\gamma)$ of k that parametrizes $\mathcal{C}$.

This result is useful in the context of algebraically optimal reparametrization of a rational curve $\mathcal{C}$. Suppose that $\mathcal{C}$ is a rational curve defined by a birational parametrization $\phi(t)$ with coefficients over $\mathbb{K}(\alpha)$, where α is algebraic of degree n over $\mathbb{K}$. The problems of deciding if $\mathcal{C}$ can be parametrized over $\mathbb{K}$ and computing such a parametrization have been studied (among others) in [1, 2, 3, 9, 11, 12]. Any birational parametrization of $\mathcal{C}$ with coefficients in $\mathbb{K}$ is of the form $\phi(\frac{at+b}{ct+d})$, where $\frac{at+b}{ct+d} \in \mathbb{K}(\alpha)(t)$. Computing a valid linear fraction $\frac{at+b}{ct+d}$ that reparametrices ϕ over $\mathbb{K}$ is at least as hard as computing a point in $\mathcal{C} \cap \mathbb{K}^N$. A parametric version of Weil's descente method is proposed in [2] to transform the curve $\mathcal{C}$ to a witness variety where the problem is thought to be easier. It is known [2, 3] that $\mathcal{C}$ is parametrizable over $\mathbb{K}$ if and only if the witness variety is a special curve called α-hypercircle. These α-hypercircles have many interesting geometric properties [8], some of them related with the algebraic extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$.

An α-hypercircle is a curve that depends on $\mathbb{K}$ and α. In this article we prove that, if $\mathcal{C}$ is defined over $\mathbb{K}$, then the associated witness variety to ϕ is a curve that is always a hypercircle for $\mathbb{K}(\beta)$ and α, where β is algebraic of degree at most 2 over $\mathbb{K}$ and $[\mathbb{K}(\beta, \alpha) : \mathbb{K}(\beta)] = [\mathbb{K}(\alpha) : \mathbb{K}] = n$. As a consequence we can derive the following property of hypercircles: let r be the geometric degree of the hypercircle associated to ϕ. Then there exists an intermediate field $\mathbb{K} \subseteq \mathbb{K}(\gamma) \subseteq \mathbb{K}(\alpha)$, $[\mathbb{K}(\gamma) : \mathbb{K}] = r$, and an affine change of variable $at + b$ such that $\phi(at + b) \in \mathbb{K}(\gamma)(t)$. Moreover, this field $\mathbb{K}(\gamma)$ is of minimal degree among the fields obtained by an affine change of parameter $\phi(at + b)$.

$$[\mathbb{K}(\gamma) : \mathbb{K}] \leq [\mathbb{K}(\text{coeffs}(\phi(at + b))) : \mathbb{K}]$$

The main advantage is that computing γ, $at + b$ and points in $\mathcal{C} \cap \mathbb{K}(\gamma)^N$ is relatively easy compared to the problem of finding points in $\mathcal{C} \cap \mathbb{K}^N$.

1.1 Preliminaries

Let $\mathbb{K}$ be a characteristic zero field, $\mathbb{F}$ its algebraic closure. Let $\mathcal{C} \subseteq \mathbb{F}^N$ be an irreducible algebraic variety over $\mathbb{F}$. We say that $\mathbb{K}$ is a *field of definition* of $\mathcal{C}$ if $\mathcal{C}$ can be expressed as the set of common zeros in $\mathbb{F}^N$ of an ideal in $\mathbb{K}[x_1, \ldots, x_N]$.

From an algebraic point of view, consider the canonical ring inclusions $\mathbb{K} \subseteq \mathbb{K}[x_1, \ldots, x_N] \subseteq \mathbb{F}[x_1, \ldots, x_N]$. Let $P \in \text{Spec}(\mathbb{F}[x_1, \ldots, x_N])$ be a prime ideal. Denote by

$$\mathbb{K}(P) = Frac\frac{\mathbb{K}[x_1, \ldots, x_N]}{P^c}$$

where P^c is the contracted ideal $P^c = P \cap \mathbb{K}[x_1, \ldots, x_n]$. Consider the induced field extensions

$$\mathbb{K} \subseteq \mathbb{K}(P) \subseteq \mathbb{F}(P)$$

Recall that a finitely generated extension of fields $A \subseteq B$ is *regular* if the extension is separable and A is algebraically closed in B (cf. [14]). Also, an ideal $P \in \operatorname{Spec}(\mathbb{K}[x_1, \ldots, x_N])$ is called *absolutely prime* if P^e is prime in $\mathbb{L}[x_1, \ldots, x_N]$ for any extension $\mathbb{L}$ of $\mathbb{K}$.

Proposition 1.1. *The following statements are equivalent:*

1. *P has a set of generators with coefficients in $\mathbb{K}$.*

2. *$P = P^{ce}$ is an extended ideal for $\mathbb{K}[x_1, \ldots, x_N] \subseteq \mathbb{F}[x_1, \ldots, x_N]$.*

3. *P^{ce} is prime in $\mathbb{F}[x_1, \ldots, x_N]$.*

4. *P^c is absolutely prime.*

5. *The field extension $\mathbb{K} \subseteq \mathbb{K}(P)$ is regular.*

Proof. It follows easily form the results in [14] Ch VII §11. $\quad\square$

If these properties hold, we say that $\mathbb{K}$ is *a field of definition* of P. Obviously, $\mathbb{F}$ is always a field of definition of any P and any extension of a field of definition is again a field of definition. It is known that there is a minimum field of definition k of P with respect to inclusion. This field k is *the* field of definition of P. This field is always finitely generated over $\mathbb{Q}$.

Definition 1.2. Let $P \in \operatorname{Spec}(\mathbb{F}[x_1, \ldots, x_N])$, $Q \in \operatorname{Spec}(\mathbb{F}[y_1, \ldots, y_M])$ be two prime ideals. A $\mathbb{K}$-*isomorphism* of $\mathbb{F}(P)$ and $\mathbb{F}(Q)$ is an isomorphism of fields ϕ such that $\phi|_{\mathbb{F}} = id$, $\phi([x_i]) \in \mathbb{K}(Q)$, $\phi^{-1}([y_j]) \in \mathbb{K}(P)$, $1 \leq i \leq N$, $1 \leq j \leq M$. In this case we say that the varieties defined by P and Q are $\mathbb{K}$-*birational*.

Definition 1.3. Let P define a rational curve. That is

$$\mathbb{F}(P) \cong \mathbb{F}(t)$$

We say that $\mathbb{K}$ is *a field of parametrization* of P if there is a $\mathbb{K}$-isomorphism between $\mathbb{F}(P)$ and $\mathbb{F}(t)$. This isomorphism is called a $\mathbb{K}$-*parametrization*. We say in this case that the curve is $\mathbb{K}$-*parametrizable*.

If P is $\mathbb{K}$-parametrizable, then it follows that $\mathbb{K}(P) \cong \mathbb{K}(t)$ by an isomorphism that is the identity in $\mathbb{K}$. Then, since $\mathbb{K} \subseteq \mathbb{K}(t)$ is regular, by Proposition 1.1, $\mathbb{K}$ is a field of definition.

But it could happen that $\mathbb{K}$ is a field of definition of P without being a field of parametrization. Then, it is known [4] that there exists at least an element η that is quadratic over $\mathbb{K}$ such that $\mathbb{K}(\eta)$ is a field of parametrization of P. So, if the field of definition k of P is not a field of parametrization, there are always minimal fields of parametrization under inclusion that are quadratic extensions of k.

Example 1.4. *Let $P = (x + iy), Q = (x^2 + y^2 + 1) \subseteq \mathbb{C}[x, y]$, $\mathbb{K} = \mathbb{R}$. Then $P^c = (x^2 + y^2)$, the extension $\mathbb{R} \subseteq \mathbb{R}(P)$ is not regular, because $(x/y)^2 + 1 = 0$, x/y is algebraic over $\mathbb{R}$. In fact*

$$\phi: \quad \begin{array}{ccc} Frac\ \mathbb{R}[x, y]/(x^2 + y^2) & \to & \mathbb{C}(x) \\ [x] & \mapsto & x \\ [y] & \mapsto & ix \end{array}$$

*is an isomorphism of fields. So $\mathbb{R}$ is not a field of definition of P. On the other hand, $\mathbb{R}$ is a field of definition of Q but $\mathbb{R}(Q)$ is not a real field, so it is not isomorphic to $\mathbb{R}(t)$ and $\mathbb{R}$ is not a field of parametrization of Q (cf. [7]). If we look for the fields of parametrization of Q that contains $\mathbb{R}$, the only possibility is the complex field. This is not a contradiction with the aim to prove that there are infinitely many minimal fields of parametrization, because $\mathbb{R}$ is not **the** field of definition of Q. We will prove that there are infinitely many quadratic fields over $\mathbb{Q}$ that parametrices Q.*

Proposition 1.5. *Let $P \in \mathrm{Spec}(\mathbb{F}[x_1, \ldots, x_N])$ define a curve, let $\mathbb{K}$ be a field of definition of P then P is $\mathbb{K}$-birational to a plane curve Q defined over $\mathbb{K}$.*

Proof. We write the classical proof for completeness. Since P defines a curve, $\mathbb{K}(P)$ is of transcendence degree 1 over $\mathbb{K}$. Let $x = g_1([x_1], \ldots, [x_N]) \in P$ be transcendent over $\mathbb{K}$. Then $\mathbb{K}(x) \subseteq \mathbb{K}(P)$ is algebraic and finite, so there is an element $y = g_2([x_1], \ldots, [x_N])$ algebraic over $\mathbb{K}(x)$ such that $\mathbb{K}(x, y) = \mathbb{K}(P)$. Taking the minimal polynomial of y over $\mathbb{K}(x)$ and clearing denominators, we get an equation $f(x, y)$ such that $Frac\mathbb{K}[x, y]/(f(x, y)) \cong \mathbb{K}(P)$. Let Q be the curve defined by $f(x, y)$. Clearly Q is defined over $\mathbb{K}$ and the isomorphism

$$\phi: \quad \begin{array}{ccc} \mathbb{F}(Q) & \to & \mathbb{F}(P) \\ [x] & \mapsto & g_1([x_1], \ldots, [x_N]) \\ [y] & \mapsto & g_2([x_1], \ldots, [x_N]) \end{array}$$

is a $\mathbb{K}$-isomorphism. $\qquad \square$

Theorem 1.6 (Hilbert-Hurwitz). *Let $P = (f(x, y)) \in \mathrm{Spec}(\mathbb{F}[x, y])$ define a rational curve defined over $\mathbb{K}$, $\deg(f) = d > 2$, $f(x, y) \in \mathbb{K}[x, y]$. Then the curve defined by P is $\mathbb{K}$-birational to a curve of degree $d - 2$ defined over $\mathbb{K}$.*

Proof. [6, 12] $\qquad \square$

2 The number of fields of parametrization

By the previous results, every rational curve $\mathcal{C}$ defined over $\mathbb{K}$ is $\mathbb{K}$-birational to a plane curve $\mathcal{C}'$ of degree at most 2. If $\mathcal{C}'$ is a line or a conic that is $\mathbb{K}$-parametrizable, then $\mathcal{C}$ is $\mathbb{K}$-parametrizable. More generally, if $\mathbb{L}$ is a field of parametrization of C' and $\mathbb{K} \subseteq \mathbb{L}$ then $\mathbb{L}$ is a field of parametrization of $\mathcal{C}$. Using standard projective transformations, we can reduce the problem of deciding if $\mathcal{C}$ is parametrizable over $\mathbb{K}$ to a plane conic defined by a polynomial

4

of the form $(ax^2 + by^2 + c)$. In the general case, one would use the primitive element theorem to find a plane curve birational to the given curve and then use Hilbert-Hurwitz to compute a conic birational to it. It is worthy to comment that we may change the field of definition of the curve during this process. For example, the curve defined by $(x - \sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})[x, y]$ is defined over $\mathbb{Q}(\sqrt{2})$ and it is $\mathbb{Q}(\sqrt{2})$-birational with $(0) \subseteq \mathbb{Q}[x]$. In this case the field of definition of the second variety is $\mathbb{Q}$ and not $\mathbb{Q}(\sqrt{2})$. So, we have to be flexible with what fields of definition we are dealing with and not work only with the field of definition of the original curve. But, in order to avoid cases such as Example 1.4, we cannot take too big fields. To solve this problem, we will restrict to fields of definition $\mathbb{K}$ that are finitely generated over $\mathbb{Q}$ (as a field) and are not fields of parametrization. We may suppose, without loss of generality, that $\mathbb{K} = \mathbb{Q}(y_1, \ldots, y_u)(\beta)$, where $y_1, \ldots, y_u$ are indeterminates and β is algebraic of degree v over $\mathbb{Q}(y_1, \ldots, y_u)$. Let $\mathbb{E}$ be the integral closure of the ring $R = \mathbb{Z}[y_1, \ldots, y_u]$ in $\mathbb{K}$. Without loss of generality, we may suppose that β is integral over R and that $\beta = \beta_1, \ldots, \beta_v$ are the conjugates of β in $\mathbb{F}$. First, we need some elementary properties of these rings.

Lemma 2.1. $\mathbb{E}$ *is a finitely generated R-module.*

Proof. This is a well known result that follows from the fact that the discriminant D of β is a universal denominator for the ring of integers, $D\mathbb{E} \subseteq <1, \beta, \ldots, \beta^{v-1} >$ (See [5]). We know that $\{1, \beta, \beta^2, \ldots, \beta^{v-1}\}$ is a base of the $\mathbb{Q}(y_1, \ldots, y_u)$-vectorial space $\mathbb{K}$. Let $\mathbb{D}$ be the integral closure of R in $\mathbb{F}$. Take $a \in \mathbb{E}$, then, $a = a_0 + a_1\beta + \ldots + a_{v-1}\beta^{v-1}$, $a_i \in \mathbb{Q}(y_1, \ldots, y_u)$. Let $a = b_1, \ldots, b_v$ be the conjugates of a in $\mathbb{D}$ defined by:

$$\begin{pmatrix} b_1 \\ \vdots \\ b_v \end{pmatrix} = \begin{pmatrix} 1 & \beta & \ldots & \beta^{v-1} \\ & & \ldots\ldots & \\ 1 & \beta_v & \ldots & \beta_v^{v-1} \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{v-1} \end{pmatrix}$$

with coefficient matrix B. Multiplying by the adjoint matrix (whose elements are in $\mathbb{D}$, that is, are integral elements) and $det(B)$ we obtain:

$$det(B) adj(B) \begin{pmatrix} b_1 \\ \vdots \\ b_v \end{pmatrix} = det(B)^2 \begin{pmatrix} a_0 \\ \vdots \\ a_{v-1} \end{pmatrix}$$

The left part of the equation belongs to $\mathbb{D}$. Note that $D = det(B)^2 = \text{disc}(\beta) \in R$ belongs to the base ring. So, every Da_i is integral over R and belongs to $\mathbb{Q}(y_1, \ldots, y_u)$. Since R is a UFD, it is integrally closed in its field of fractions, so $Da_i \in R$.

To sum up, if $a = a_0 + a_1\beta + \ldots + a_{v-1}\beta^{v-1} \in \mathbb{E}$, then $Da_i \in R, 0 \le i \le v-1$. So $\mathbb{E} \subseteq < 1/D, \beta/D, \ldots, \beta^{v-1}/D > \subseteq \mathbb{K}$ a finitely generated R-module. Since R is noetherian, $\mathbb{E}$ is also finitely generated. $\square$

Now, we define a multiplicative function in order to have some control on divisibility in $\mathbb{E}$.

Definition 2.2. Consider the map $N_1 : \mathbb{Z}[y_1, \ldots, y_u] \to \mathbb{N}$ defined by:

$$N_1(x) = \begin{cases} |x| & \text{if } x \in \mathbb{Z} \\ 2 & \text{if } x \notin \mathbb{Z}, x \text{ irreducible} \\ 2^k|c| & \text{if } x = cf_1 \ldots f_k, c \in \mathbb{Z}, f_i \notin \mathbb{Z} \text{ irreducible} \end{cases}$$

N_1 is a multiplicative map such that $N_1(x) = 0 \leftrightarrow x = 0$, $N_1(x) = 1$ if and only if $x \in \{1, -1\}$.

Define $N_2 : \mathbb{E} \to \mathbb{Z}[y_1, \ldots, y_u]$ as the restriction of the norm associated to the algebraic extension $\mathbb{Q}(y_1, \ldots, y_u) \subseteq \mathbb{K}$. Let $N = N_1 \circ N_2 : \mathbb{E} \to \mathbb{N}$.

Lemma 2.3. *In the previous conditions:*

- $N(ab) = N(a)N(b)$, N *is multiplicative.*

- $N(x) = 0$ *if and only if* $x = 0$.

- $N(x) = 1$ *if and only if* x *is a unit in* $\mathbb{E}$.

- *If* $A, B \in \mathbb{E}^*$ *and* $N(A) \nmid N(B)$ *then* $A \nmid B$.

Proof. N is the composition of multiplicative maps, so it is multiplicative. If $x = 0$, then it is clear that $N(x) = 0$. If $N(x) = 0$, then $N_1(N_2(x)) = 0$, so $N_2(x) = 0$ and $x = 0$. If x is a unit in $\mathbb{E}$ then $1 = N(1) = N(xx^{-1}) = N(x)N(x^{-1})$ so $N(x)$ is a natural number that divides 1, it has to be 1. Reciprocally, if $N(x) = 1$, then $N_2(x) = \pm 1$. The minimal polynomial of x over $\mathbb{Z}[y_1, \ldots, y_u]$ is of the form $x^s + a_1 x^{s-1} + \ldots + a_{s-1}x \pm 1$, $s \geq 1$. So, in $\mathbb{E}$, $x(x^{s-1} + a_{s-1}x^{s-2} + \ldots + a_{s-1}) = \mp 1$ and x is a unit. The last item follows from the multiplicativity of N. $\qquad\square$

Lemma 2.4. *Let* $x \in \mathbb{E}^*$, *let* $p \in \mathbb{Z}$ *be an integer prime such that* $p > N(x)$, *then* $x \notin \sqrt{p\mathbb{E}}$ *and there is a maximal ideal* m_p *in* $\mathbb{E}$ *such that* $p \in m_p$, $x \notin m_p$.

Proof. If $p > N(x)$, $x \neq 0$, then $p \nmid N(x)$ in $\mathbb{Z}$, so $N(p) = p^v \nmid N(x^K)$ and $p \nmid x^K$ in $\mathbb{E}$. Thus $x \notin \sqrt{p\mathbb{E}}$. In this context, consider the ring of fractions $x^{-1}\mathbb{E}$ whose denominators are the powers of x. $(p)^e$ is a proper ideal in $x^{-1}\mathbb{E}$. Let P be a maximal ideal of $x^{-1}\mathbb{E}$. Its contraction is a prime ideal containing p but not x^N. Consider the map

$$\phi : \mathbb{E}/P^c \to x^{-1}\mathbb{E}/P$$

such that $\phi(a + P^c) = a/1 + P$. ϕ is well defined and injective. Now, the field of the right is of characteristic p and is a finitely generated $\mathbb{F}_p$-algebra, so it has to be an algebraic extension of $\mathbb{F}_p$. It follows that $\mathbb{E}/P^c$ is a finite domain, so a field and P^c is a maximal ideal such that $p \in P^c$, $x \notin P^c$. $\qquad\square$

Lemma 2.5. *Let* m *be a maximal ideal in* $\mathbb{E}$ *such that* $char(\mathbb{E}/m) = p \neq 2$, $p \equiv 1 \mod 4$. *Let* $e \not\equiv 0 \mod m$. *Then, there is a* $n \in \mathbb{E}$ *such that* $1 + en^2$ *is not a square mod* m.

Proof. $\mathbb{E}/m \cong \mathbb{F}_{p^q}$, the field of p^q elements. Suppose that $1 + en^2$ is always a square mod m. Then $[1+ex]$ is a bijection of $\mathbb{F}_{p^q}$ such that maps the squares into themselves. It follows that it is a bijection among the squares. In particular, there is a $[n]$ such that $[1 + en^2] = [0]$ a square. As $p \equiv 1 \mod 4$, $[-1]$ is a square in $\mathbb{F}_{p^q}$. So $[e]^{-1} = [-n^2]$ is a square and also $[e]$ is a square. Thus, $[1+x]$ is a bijection on the set of squares. But this is impossible. If this where the case, every element of $\mathbb{F}_p$ would be a square and $[x]$ is a square if and only if $[x+i]$ is a square for every $i \in \mathbb{F}_p$. In $\mathbb{F}_{p^q}$ there are $\frac{p^q+1}{2}$ squares. The equivalence relation $a \sim b \leftrightarrow a - b \in \mathbb{F}_p$ produces a partition of $\mathbb{F}_{p^q}$ into equivalence classes, each one containing exactly p elements. In a equivalence class, either every element is a square or none is. Hence, it follows that the number of squares is divisible by p, while $(p^r + 1)/2$ is not. $\qquad\square$

Note that depending on the maximal m, it may happen that necessarily $n \notin \mathbb{Z}$ in the Lemma. In order to prove that $\mathcal{C}$ has infinitely many fields of parametrization, we suppose without loss of generality that $\mathcal{C}$ is a plane conic defined by the polynomial $ax^2 + by^2 + c$, where $a, b, c \in \mathbb{E}^*$. Suppose that the conic does not have points with coefficients in $\mathbb{K}$. Let $n \in \mathbb{E}$ be such that $a + bn^2 \neq 0$. The intersection of the conic and the line $y = nx$ provides the points

$$\left(\pm\sqrt{\frac{-c}{a + bn^2}}, \pm n\sqrt{\frac{-c}{a + bn^2}} \right)$$

that have coefficients in $\mathbb{K}(\sqrt{\frac{-c}{a+bn^2}})$. This is a field of parametrization of $\mathcal{C}$.

Lemma 2.6. *Let $n \neq m \in \mathbb{K}^*$, such than $a + bn^2 \neq 0 \neq a + bm^2$. Then, $\mathbb{K}(\sqrt{\frac{-c}{a+bn^2}}) = \mathbb{K}(\sqrt{\frac{-c}{a+bm^2}})$ if and only if $\frac{a+bn^2}{a+bm^2}$ is a square in $\mathbb{K}$.*

Proof. Straightforward. $\qquad\square$

Theorem 2.7. *In the previous conditions. There is an infinite set $S \subseteq \mathbb{E}$ such that for all $p \neq q \in S$, $a + bp^2 \neq 0$, $a + bq^2 \neq 0$ and $\frac{a+bp^2}{a+bq^2}$ is not a square in $\mathbb{K}$.*

Proof. Let P be an enumeration of the integer primes $p \in \mathbb{Z}$ such that $p \equiv 1 \mod 4$, $a + bp^2 \neq 0$, $p > N(ab)$. The set P is infinite. To each prime p_i we associate to it a maximal ideal m_i such that $p \in m_i$, $ab \notin m_i$. It is clear that all these maximal ideals are different. We are going to construct the set S inductively from P. Define $S_1 = \{p_1\}$, suppose that we have defined a set $S_i = \{n_1, \ldots, n_i\}$ such that:

- $n_j \in m_{p_j}$, $1 \leq j \leq i$

- $a + bn_j^2 \neq 0$, $1 \leq j \leq i$

- If $j \neq k$, $\frac{a+bn_j^2}{a+bn_k^2}$ is not a square in $\mathbb{K}$.

7

Then, we define S_{i+1} as follows. For $1 \leq j \leq i$, $[a + bn_j^2] = [a] \mod m_j$, so $\frac{[a+bx^2]}{[a+bn_j^2]} = [1] + [b][a]^{-1}[x^2] \mod m_j$. By Lemma 2.5, there is a $q_j \in \mathbb{E}$ such that $[1] + [b][a]^{-1}[q_j^2]$ is not a square mod m_j. Now, by the Chinese reminder theorem, as the ideals $m_1, \ldots, m_{i+1}$ are pairwise comaximal, there is an element n_{i+1} such that $n_{i+1} \equiv q_j \mod m_j$, $1 \leq j \leq i$; $n_{i+1} \equiv 0 \mod m_{i+1}$. Then $n_{i+1} \in m_{i+1}$. As $[1] + [b][a^{-1}][n_{i+1}^2]$ is not a square mod m_j, $1 \leq j \leq i$ then, any representative of this class in $\mathbb{E}$ is not a square in $\mathbb{E}$. However, we want to prove that $\frac{a+bn_{i+1}^2}{a+bn_j^2}$ is not a square in $\mathbb{K}$ instead.

Consider the extension of rings $\mathbb{E} \subseteq \mathbb{E}' = (a + bn_j^2)^{-1}\mathbb{E} \subseteq \mathbb{K}$. Since $\mathbb{E}$ is integrally closed in $\mathbb{K}$, then $\mathbb{E}'$ is also integrally closed in $\mathbb{K}$. So, an element $x \in \mathbb{E}'$ is a square in $\mathbb{E}'$ if and only if it is a square in $\mathbb{K}$. By construction, $\frac{a+bn_{i+1}^2}{a+bn_j^2}$ is not a square in $\mathbb{E}'/m_j\mathbb{E}'$, so it is not a square in $\mathbb{E}'$ and hence, it is not a square in $\mathbb{K}$.

We define $S_{i+1} = \{n_1, \ldots, n_{i+1}\}$. □

Corollary 2.8. *Let $\mathcal{C} = \{ax^2 + by^2 + c = 0\}$, $a, b, c \in \mathbb{E}^*$ be an (absolutely) irreducible conic that has no points with coordinates in $\mathbb{K}$, then there are infinitely many distinct quadratic fields over $\mathbb{K}$ such that the curve has points defined over them.*

Proof. Let S be the set defined in Theorem 2.7, by Lemma 2.6 we have that the fields

$$\mathbb{K}\left(\sqrt{\frac{-c}{a + bn^2}}\right), n \in S$$

are pairwise distinct and $\mathcal{C}$ has points defined over them □

Corollary 2.9. *Let $\mathbb{K}$ be a field of definition of a rational curve $\mathcal{C}$ such that $\mathbb{K}$ is finitely generated over $\mathbb{Q}$. If $\mathcal{C}$ is not parametrizable over $\mathbb{K}$, then $\mathcal{C}$ has infinitely many distinct fields of parametrization that are quadratic over $\mathbb{K}$. In particular, if $\mathcal{C}$ is not parametrizable over its minimum field of definition k, then there are infinitely many minimal fields of parametrization that are quadratic over k.*

This Corollary is equivalent to the following fact. Let $\mathcal{C}$ be a genus zero curve defined over $\mathbb{K}$. Suppose that $\mathcal{C}$ is not parametrizable over $\mathbb{K}$. Then, for any field of parametrization $\mathbb{K}(\alpha)$, where α is algebraic over $\mathbb{K}$, there is a quadratic element γ over $\mathbb{K}$ such that $\mathbb{K}(\gamma)$ is a field of parametrization of $\mathcal{C}$ and $\mathbb{K}(\alpha) \cap \mathbb{K}(\gamma) = \mathbb{K}$.

The main disadvantage of the method in Theorem 2.7 is that it is not constructive, because of the use of the maximal ideals m_i. We can give a constructive proof of the theorem whenever our base ring R is the ring of integers $\mathbb{Z}$ and $\mathbb{K} = \mathbb{Q}(\alpha)$ is an algebraic number field. In this case, the set S can be taken as a set of integer primes.

Theorem 2.10. *Given $a, b \in \mathbb{Z}^*$, there is an infinite set S such that: every element in S is a prime $p \equiv 1 \mod 4$, $p \nmid ab$, $a + bp^2 \neq 0$ and, if $p, q \in S$, then*

$$f(p, q) = \frac{a + bp^2}{a + bq^2}$$

is not a square in $\mathbb{Q}$.

Proof. As in Theorem 2.7, we will define S inductively, starting from $S_1 = \{p_1\}$ with p_1 any prime $p_1 \equiv 1 \mod 4$ such that $p_1 \nmid ab$. Note that $a + bp_1^2 \neq 0$. Suppose we have defined a set $S_i = \{p_1, \ldots, p_i\}$ such that p_j is prime, $p_j \equiv 1 \mod 4$, $p_j \nmid ab$, and if $k \neq j$ then $\frac{a+bp_k^2}{a+bp_j^2}$ is not a square in $\mathbb{Q}$. We want to construct the set S_{i+1}. Consider the residual polynomial in the variable n with coefficients in $\mathbb{F}_{p_j}$

$$[a + bn^2][a + bp_j^2]^{-1} = [1] + [a]^{-1}[bn^2] = [1 + en^2].$$

Note that $[e] \neq [0]$ is well defined because $p_j \nmid ab$. Let n_j be such that such that $[1 + en_j^2]$ is not a square. Let p be a prime such that $p \equiv 1 \mod 4$, $p \equiv n_j \mod p_j$, $(p, ab) = 1$. This prime always exists: from the Chinese remainder theorem, we can compute the unique class $N \mod 4p_1 \cdots p_i$ such that verifies the previous modular equations. As N is a unit $\mod 4p_1 \cdots p_i$, we can apply Dirichlet's theorem and find a prime $p \equiv N \mod 4p_1 \cdots p_i$ such that, in addition, it does not divide ab. Take $p_{i+1} = p$ in S_{i+1}. By construction, $p \equiv 1 \mod 4$, $p \nmid ab$ and, in $\mathbb{Z}/p_j\mathbb{Z}$

$$[a + bp^2][a + bp_j^2]^{-1} = [a + bm_j^2][a + bp_j^2]^{-1} = [1 + em_j^2]$$

which is not a square $\mod p_j$, so $\frac{a+bp^2}{a+bp_j^2}$ is not a square in $\mathbb{Q}$, $1 \leq j \leq i$. $\square$

Note that, in this case, the set obtained differs from the set obtained in Theorem 2.7. Because this set is a set on integer primes, while the set $S = \{q_i\}$ obtained using Theorem 2.7 is such that q_i is a multiple if the i-th integer prime which is $\equiv 1 \mod 4$.

Example 2.11. *Let $\mathcal{C} = x^2 + y^2 - 6 = 0$ which does not have points in $\mathbb{Q}^2$. We look for a set of integers such that $\frac{1+n^2}{1+m^2}$ is never a square. Take $p_1 = 5$. Now we search a $[n]$ such that $1 + n^2$ is not a square $\mod 5$. For example $1 + 1^2 = 2$ is not a square $\mod 5$. Now compute a prime p_2 such that:*

$$p_2 \equiv 1 \mod 4, \quad p_2 \equiv 1 \mod 5$$

By the Chinese reminder Theorem. $p_2 \equiv 1 \mod 20$ and, we can take, for example $p_2 = 41$. Now we need to compute p_3, we impose $1 + n^2$ not to be a square $\mod 41$, the first non square of this form is $1 + 4^2 = 17$. Again we have the following system of residual equations

$$p_3 \equiv 1 \mod 4, \ p_3 \equiv 1 \mod 5, \ p_3 \equiv 4 \mod 41$$

9

So, this time, $p_3 \equiv 701 \mod 820$. we can take $p_3 = 701$. Applying again this method, we arrive that the next prime must be $p_4 \equiv 266381 \mod 574820$ and, in particular we can take, $p_4 = 266381$. That is, the intersection of $\mathcal{C}$ with the lines $y = 5x$, $y = 41x$, $y = 701x$ and $y = 266381x$ gives four different quadratic fields of parametrization of the conic. In this case, we obtain:

$$\mathbb{Q}\left(\sqrt{\frac{3}{13}}\right), \mathbb{Q}(\sqrt{3}), \mathbb{Q}\left(\sqrt{\frac{3}{245701}}\right), \mathbb{Q}\left(\sqrt{\frac{3}{35479418581}}\right)$$

If we apply instead Theorem 2.7 we will get that the first terms of S are:

$$S = \{5, 26, 391, 4031, 175306, 9276086, \ldots\}$$

3 Any witness variety is a hypercircle

Let $\mathcal{C} \subseteq \mathbb{F}^N$ be a rational curve defined by the birational parametrization $(\phi_1(t), \ldots, \phi_N(t))$, where $\phi_i(t) \in \mathbb{K}(\alpha)(t)$. Suppose that the rational functions are written with common denominator g, $\phi_i(t) = f_i/g$, $1 \leq i \leq N$, $\gcd(f_1, \ldots, f_N, g) = 1$ and that α is algebraic of degree n over $\mathbb{K}$.

Perform Weil's descente parametric version presented in [2], substitute $t = \sum_{i=0}^{n-1} \alpha^i t_i$, where t_i are new variables. Rewrite:

$$\phi_j \left(\sum_{i=0}^{n-1} \alpha^i t_i \right) = \sum_{i=0}^{n-1} \alpha^i \psi_{ij}(t_0, \ldots, t_{n-1}), \psi_{ij} = \frac{F_{ij}}{\delta} \in \mathbb{K}(t_0, \ldots, t_{n-1})$$

Let $\mathcal{Z}$ be the Zariski closure of

$$\{F_{ij} = 0 \mid 1 \leq i \leq n-1, \ 1 \leq j \leq N\} \setminus \{\delta = 0\} \subseteq \mathbb{F}^n.$$

$\mathcal{Z}$ is called the *witness variety* of the parametrization ϕ.

Theorem 3.1. *With the previous notation:*

- *Dim $\mathcal{Z} \leq 1$.*

- *$\mathcal{Z}$ has at most one 1-dimensional component.*

- *$\mathbb{K}$ is a field of definition of $\mathcal{C}$ if and only if Dim $\mathcal{Z} = 1$.*

- *$\mathcal{C}$ is parametrizable over $\mathbb{K}$ if and only if the 1-dimensional component of $\mathcal{Z}$ is parametrizable over $\mathbb{K}$.*

Proof. [2, 3, 13] □

So, the problem of parametrizing $\mathcal{C}$ over $\mathbb{K}$ can be translated to the problem of parametrizing the one-dimensional component of the witness variety over $\mathbb{K}$. The interesting thing is that this problem is related with the study of hypercircles:

Definition 3.2. Let $\frac{at+b}{ct+d} \in \mathbb{K}(\alpha)(t)$ represents a $\mathbb{K}(\alpha)$-isomorphism of $\mathbb{F}(t)$, $a, b, c, d \in \mathbb{K}(\alpha)$, $ad - bc \neq 0$. Write

$$\frac{at+b}{ct+d} = \psi_0(t) + \alpha\psi_1(t) + \cdots + \psi_{n-1}(t)$$

where $\psi_i(t) \in \mathbb{K}(t)$. The α-*hypercircle* associated to $\frac{at+b}{ct+d}$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ is the parametric curve in $\mathbb{F}^n$ given by the parametrization $(\psi_0, \ldots, \psi_{n-1})$.

Usually, if the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ and the primitive element α are assumed, we could just talk about the witness variety of ϕ or the hypercircle associated to $\frac{at+b}{ct+d}$. But, since we will explicitly change the algebraic extension to consider or the primitive element, we will try to avoid this language as it can be misleading.

It can be easily proved that fixed $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ and a primitive element α, two linear fraction $u = \frac{at+b}{ct+d}$, $v = \frac{a't+b'}{c't+d'} \in \mathbb{K}(\alpha)(t)$ define the same hypercircle if and only there is a linear fraction $w = \frac{a''t+b''}{c''t+d''} \in \mathbb{K}(t)$ such that $u(t) = v(w(t))$.

Note also that if $c = 0$ in the linear fraction, then the hypercircle is a line parametrizable over $\mathbb{K}$. Anyway, by composing on the right by an appropriate linear fraction $w \in \mathbb{K}(t)$, we can always suppose that the associated unit of the hypercircle is of the form $\frac{at+b}{t+d}$ $(c = 1)$. We will suppose that this is the case from now on unless otherwise specified.

Now we show some other useful facts about hypercircles. The proofs of these facts can be checked in [8]

Lemma 3.3. *Let $\mathcal{U}$ be the α-hypercircle associated to $\frac{at+b}{t+d} \in \mathbb{K}(\alpha)(t)$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Then, the geometric degree of $\mathcal{U}$ equals $[\mathbb{K}(d) : \mathbb{K}]$*

Definition 3.4. Let $\mathcal{U}$ be an α-hypercircle, if the geometric degree of $\mathcal{U}$ equals $n = [\mathbb{K}(\alpha) : \mathbb{K}]$ then $\mathcal{U}$ is called a *primitive* hypercircle. i.e. If the d of an associated unit $\frac{at+b}{t+d}$ is a primitive element for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$.

Lemma 3.5. *Let $u(t) = \frac{at+b}{t+d}$ be a unit and $\mathcal{U}$ its associated α-hypercircle for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Then $\mathcal{U}$ is affinely equivalent over $\mathbb{K}$ to the α-hypercircle $\mathcal{U}^\star$ generated by $u^\star(t) = \frac{1}{t+d}$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$.*

Theorem 3.6. *Let $\mathcal{U}$ be the non-primitive α-hypercircle associated to $u(t) = \frac{at+b}{t+d} \in \mathbb{K}(\alpha)(t)$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Let $\mathcal{V}$ be the d-hypercircle associated to the unit $\frac{1}{t+d}$ for the extension $\mathbb{K} \subseteq \mathbb{K}(d)$. Then, there is an affine inclusion from $\mathbb{F}^r$ to $\mathbb{F}^n$, defined over $\mathbb{K}$, that maps $\mathcal{V}$ onto $\mathcal{U}$.*

Proposition 3.7. *Let $M_\alpha(t)$ be the minimal polynomial of α over $\mathbb{K}$. Let $m_\alpha(t) = \frac{M_\alpha(t)}{t-\alpha} = \sum_{i=0}^{n-1} l_i t^i \in \mathbb{K}(\alpha)[t]$, where $l_{n-1} = 1$. Then, the points at infinity of every primitive α-hypercircle for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ are*

$$[l_0 : l_1 : \cdots : l_{n-2} : l_{n-1} : 0]$$

and its conjugates.

With the notion of hypercircle we can extend Theorem 3.1 by the following:

Theorem 3.8. *In the previous conditions, $\mathbb{K}$ is a field of parametrization of $\mathcal{C}$ and $\phi(\frac{at+b}{ct+d})$ is a parametrization of $\mathcal{C}$ over $\mathbb{K}$ if and only if the one-dimensional component of the witness variety $\mathcal{Z}$ is an α-hypercircle associated to $\frac{at+b}{ct+d}$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$.*

Proof. [2, 3] □

This Theorem will be essential in the discussion of the reparametrization algorithm, since we will use different reparametrization units, different witness varieties and, specially, different extensions.

As a Consequence of Corollary 2.9 we can prove that any witness variety is indeed a hypercircle but possibly with respect to a different algebraic extension.

Theorem 3.9. *Let $\mathcal{C}$ be a curve $\mathbb{K}$-definable, that is not $\mathbb{K}$-parametrizable, where $\mathbb{K} = \mathbb{Q}(y_1, \ldots, y_u)(\beta)$ as in Section 1.1 such that $\mathcal{C}$ is given by a $\mathbb{K}(\alpha)$-parametrization. Let $\mathcal{U}$ be the 1-dimensional component of the α-witness variety of $\mathcal{C}$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Then, there are infinitely many η, quadratic elements over $\mathbb{K}$, such that $\mathcal{U}$ is an α-hypercircle with respect to the algebraic extension $\mathbb{K}(\eta) \subseteq \mathbb{K}(\eta, \alpha)$.*

Proof. By Corollary 2.9, there are infinitely many distinct quadratic fields of parametrization $\mathbb{K}(\gamma)$ of $\mathcal{C}$. Let η be any of this quadratic element over $\mathbb{K}$ such that η does not belong to the normal closure of $\mathbb{K}(\alpha)$ over $\mathbb{K}$. In particular, there are infinitely many η satisfying this condition. The minimal polynomial of α over $\mathbb{K}(\eta)$ equals its minimal polynomial over $\mathbb{K}$. Hence, by the computational definition of the witness variety, the output is the same considering the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ or $\mathbb{K}(\eta) \subseteq \mathbb{K}(\eta, \alpha)$. But, since $\mathcal{C}$ can be parametrized over $\mathbb{K}(\eta)$, from Theorem 3.1, it follows that $\mathcal{U}$ is an α-hypercircle with respect to the extension $\mathbb{K}(\eta) \subseteq \mathbb{K}(\eta, \alpha)$. □

This result is important because hypercircles have a well known geometry. So, in particular, we automatically know many geometric properties of witness varieties, including the possible degrees, the Hilbert function, the smoothness, the structure at infinity or specific algorithms for parametrization and implicitization (See [8]).

4   Optimal Affine Reparametrization of a Curve

We have seen that any witness variety is a hypercircle for a convenient algebraic extension. In this Section, we present a method of optimal reparametrization of a curve by affine change of variables only. We will always suppose that our base field $\mathbb{K}$ is as in Section 1.1. Suppose that $\mathcal{C}$ is given by a parametrization ϕ over $\mathbb{K}(\alpha)$. We want to obtain reparametrizations of $\mathcal{C}$ by affine change of variables $t \mapsto e_1 t + e_2$ only. In this case, there is a minimum field (up to $\mathbb{K}$-isomorphism) $\mathbb{K}(\gamma)$ such that $\phi(e_1 t + e_2) \in \mathbb{K}(\gamma)(t)$. That is, there are e_1, e_2 such that $\phi(e_1 t + e_2) \in \mathbb{K}(\gamma)(t)$ and, for every pair $e_1', e_2' \in \mathbb{F}$, $e_1' \neq 0$, the field generated over $\mathbb{K}$ by the coefficients of $\phi(e_1' t + e_2')$ contains (a field isomorphic to)

$\mathbb{K}(\gamma)$. Moreover, to obtain a reparametrization over $\mathbb{K}(\gamma)$, we do not need any point over the ground field $\mathbb{K}$. This is a generalization of the reparametrization problem for polynomially parametrizable curves in [10]. We now proceed in several steps towards the algorithm.

Proposition 4.1. *Let $\mathcal{C}$ be a $\mathbb{K}$-definable curve given by a parametrization over $\mathbb{K}(\alpha)$. Let $\mathcal{U}$ be the 1 dimensional component of the α-witness variety of $\mathcal{C}$. Then, there is at least one point at infinity of $\mathcal{U}$ that admits a representation over $\mathbb{K}(\alpha)$.*

Proof. Suppose first that $\mathcal{C}$ can be parametrizable over $\mathbb{K}$. Then, by Theorem 3.1 $\mathcal{U}$ is an α-hypercircle for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ associated to a unit $\frac{at+b}{t+d} \in \mathbb{K}(\alpha)(t)$. If $\mathcal{U}$ is a primitive α-hypercircle, we have explicitly presented a point at infinity with a representation over $\mathbb{K}(\alpha)$ in Proposition 3.7. If $\mathcal{U}$ is not a primitive α-hypercircle, then, by Theorem 3.6, $\mathcal{U}$ is the image of a primitive d-hypercircle $\mathcal{U}_1$ for the extension $\mathbb{K} \subseteq \mathbb{K}(d)$ under an affine inclusion $\mathbb{F}^r \to \mathbb{F}^n$ defined over $\mathbb{K}$, $r = [\mathbb{K}(d) : \mathbb{K}]$. Hence, at least one point at infinity of $\mathcal{U}_1$ has a representation over $\mathbb{K}(d) \subseteq \mathbb{K}(\alpha)$. As the affine inclusion is defined over $\mathbb{K}$, the corresponding point at infinity of $\mathcal{U}$ also admits a representation in $\mathbb{K}(\alpha)$.

Suppose now that $\mathcal{C}$ is not $\mathbb{K}$-parametrizable. Then, by Theorem 3.9, there are infinitely many quadratic elements η over $\mathbb{K}$ such that $\mathcal{U}$ is an α-hypercircle with respect to the extension of fields $\mathbb{K}(\eta) \subseteq \mathbb{K}(\eta, \alpha)$. As there are only finite points at infinity, we conclude that there is a point p at infinity that admits a representation over infinitely many fields of the form $\mathbb{K}(\eta, \alpha)$. Necessarily, this point admits a representation over $\mathbb{K}(\alpha)$. $\square$

Let $\mathcal{C}$ be a parametric curve parametrizable over $\mathbb{K}$ but such that it is given by a parametrization over $\mathbb{K}(\alpha)$. $[\mathbb{K}(\alpha) : \mathbb{K}] = n$. Suppose that the associated hypercircle $\mathcal{U}$ to $\mathcal{C}$ is of degree $r < n$. Let $u(t) = \frac{at+b}{t+d} \in \mathbb{K}(\alpha)(t)$ be a unit associated to $\mathcal{U}$. Then $\mathbb{K}(d) \subsetneq \mathbb{K}(\alpha)$ and $[\mathbb{K}(d) : \mathbb{K}] = r$. By Theorem 3.6, $\mathcal{U}$ is $\mathbb{K}$-affinely equivalent to the primitive d-hypercircle defined by $\frac{1}{t+d}$ for the extension $\mathbb{K} \subseteq \mathbb{K}(d)$ in $\mathbb{K}^r$. Here, we present how to compute $\mathbb{K}(d)$ from the implicit equations of $\mathcal{U}$ and a reparametrization of $\mathcal{C}$ over $\mathbb{K}(d)$.

Proposition 4.2. *If $\mathcal{U}$ is the α-hypercircle associated to $\frac{at+b}{t+d}$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$, let $[a_0 : \ldots : a_{n-1} : 0]$ be a point at infinity of $\mathcal{U}$ given by a representation over $\mathbb{K}(\alpha)$, suppose that it is dehomogenized with respect to an index i. Then, $\mathbb{K}(d)$ is $\mathbb{K}$-isomorphic to $\mathbb{K}(a_0, \ldots, a_{n-1})$. In particular, there is another point at infinity $[b_0 : \ldots : b_{n-1} : 0]$ of $\mathcal{U}$, given by a representation over $\mathbb{K}(\alpha)$, dehomogenized with respect to an index i such that $\mathbb{K}(d) = \mathbb{K}(b_0, \ldots, b_{n-1})$.*

Proof. By Lemma 3.5 $\mathcal{U}$ is affinely equivalent over $\mathbb{K}$ to the α-hypercircle $\mathcal{U}_1$ associated to $\frac{1}{t+d}$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Thus, the (dehomogenized) points at infinity of $\mathcal{U}$ and $\mathcal{U}_1$ generate the same algebraic extension over $\mathbb{K}$. So, without loss of generality, we may suppose that $u(t) = \frac{1}{t+d}$ is the unit associated to $\mathcal{U}$. Let $M(t) = t^r + k_{r-1}t^{r-1} + \cdots + k_0$ be the minimal polynomial of $-d$ over $\mathbb{K}$ and let

$$m(t) = \frac{M(t)}{t+d} = l_{r-1}t^{r-1} + l_{r-2}t^{r-2} + \cdots + l_0 \in \mathbb{K}(d)[t].$$

Let $\mathcal{U}_d \subseteq \mathbb{K}^r$ be the d-hypercircle associated to $u(t)$ for the extension of fields $\mathbb{K} \subseteq \mathbb{K}(d)$. By Proposition 3.7 the points at infinity of $\mathcal{U}_d$ are $[l_0 : l_1 : \cdots : l_{r-2} : l_{r-1} : 0]$ and its conjugates. Notice that $l_{r-2} = k_{r-1} - d$, so $\mathbb{K}(l_0, \ldots, l_r) = \mathbb{K}(d)$. Finally, from Theorem 3.6 since there is an affine inclusion $\mathbb{F}^r \to \mathbb{F}^n$ that maps $\mathcal{U}_d$ onto $\mathcal{U}_1$ that is defined over $\mathbb{K}$, the field that generates the points at infinity is the same. In particular, the point $[l_0 : l_1 : \cdots : l_{r-2} : l_{r-1} : 0]$ is mapped to a point $[b_0 : \ldots : b_{n-1} : 0]$ that has a representation over $\mathbb{K}(d) \subseteq \mathbb{K}(\alpha)$. By conjugation, $\mathbb{K}(a_0, \ldots, a_{n-1})$ is isomorphic to $\mathbb{K}(b_0, \ldots, b_{n-1}) = \mathbb{K}(l_0, \ldots, l_{n-1}) = \mathbb{K}(d)$. $\qquad\square$

Once we know how to compute $\mathbb{K}(d)$, we have a method to reparametrize a curve over $\mathbb{K}(d)$.

Theorem 4.3. *Let $\mathcal{C}$ be a curve $\mathbb{K}$-definable given by a birational parametrization ϕ with coefficients in $\mathbb{K}(\alpha)$. Let $\mathcal{U}$ be the 1-dimensional component of the α-witness variety of $\mathcal{C}$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Suppose that the degree of $\mathcal{U}$ is $r < n$. Then, $\mathcal{C}$ admits a reparametrization over $\mathbb{K}(\gamma) \subseteq \mathbb{K}(\alpha)$, where $[\mathbb{K}(\gamma) : \mathbb{K}] = r$. This reparametrization can be taken affine, $t \to f_1 t + f_2 \in \mathbb{K}(\alpha)[t]$.*

Moreover, if $e_1, e_2 \in \mathbb{F}$, $e_1 \neq 0$ are algebraic, let $\phi(e_1 t + e_2)$ be another parametrization of $\mathcal{C}$ and let $\mathbb{L}$ be the field generated over $\mathbb{K}$ by the coefficients of $\phi(e_1 t + e_2)$, then

1. $[\mathbb{L} : \mathbb{K}] \geq r$.

2. $\mathbb{L}$ *contains (a field isomorphic to) $\mathbb{K}(\gamma)$.*

3. *If $[\mathbb{L} : \mathbb{K}] = r$ then $\mathbb{L}$ is isomorphic to $\mathbb{K}(\gamma)$.*

4. *There are $e_1', e_2' \in \mathbb{L}$ such that $e_1' t + e_2'$ reparametrizes ϕ over (a field isomorphic to) $\mathbb{K}(\gamma)$.*

Proof. If $\mathcal{C}$ is not parametrizable over $\mathbb{K}$, by Theorem 3.9, there is a field $\mathbb{K}(\eta)$ quadratic over $\mathbb{K}$ such that $\mathcal{U}$ is an α-hypercircle for the extension $\mathbb{K}(\eta) \subseteq \mathbb{K}(\eta, \alpha)$ and the intersection of $\mathbb{K}(\eta)$ and the normal closure of $\mathbb{K}(\alpha)$ is $\mathbb{K}$. If $\mathcal{C}$ is parametrizable over $\mathbb{K}$, then it is trivially true that there exists such a field $\mathbb{K}(\eta)$.

Since $\mathcal{U}$ is an α-hypercircle for the extension $\mathbb{K}(\eta) \subseteq \mathbb{K}(\eta, \alpha)$, there is an associated unit $u(t) = \frac{at+b}{t+d} \in \mathbb{K}(\eta, \alpha)(t)$ so that $\phi(u(t)) \in \mathbb{K}(\eta)(t)$. By Proposition 4.2, there is a point at infinity $[b_0 : \ldots : b_{n-1} : 0]$ of $\mathcal{U}$, $b_i \in \mathbb{K}(\alpha)$, $0 \leq i \leq n-1$ such that $\mathbb{K}(\eta, d) = \mathbb{K}(\eta, b_0, \ldots, b_{n-1})$. Let γ be a primitive element for the extension $\mathbb{K} \subseteq \mathbb{K}(b_0, \ldots, b_{n-1})$, $\gamma \in \mathbb{K}(\alpha)$. We have that $[\mathbb{K}(\eta, d) : \mathbb{K}(\eta)] = r$, so $[\mathbb{K}(\eta, \gamma) : \mathbb{K}(\eta)] = r$ and, since $\mathbb{K}(\eta)$ intersects the normal closure of $\mathbb{K}(\alpha)$ trivially, we have that $[\mathbb{K}(\gamma) : \mathbb{K}] = r$.

Let us perform Weil's construction again but now with respect to the extension $\mathbb{K}(b_0, \ldots, b_{n-1}) \subseteq \mathbb{K}(\alpha)$ with primitive element α. Since the minimal polynomial of α over $\mathbb{K}(\gamma)$ equals the minimal polynomial of α over $\mathbb{K}(\eta, \gamma)$, we get that the witness variety $\mathcal{U}'$ of $\mathcal{C}$ for the extension $\mathbb{K}(\gamma) \subseteq \mathbb{K}(\alpha)$ equals the witness variety of $\mathcal{C}$ for the extension $\mathbb{K}(\eta, \gamma) = \mathbb{K}(\eta, d) \subseteq \mathbb{K}(\eta, \alpha)$.

Now $\frac{at+b}{t+d}$ reparametrizes ϕ over $\mathbb{K}(\eta)$, so $\frac{at+b}{t+d}$ is also an associate unit of $\mathcal{U}'$ for the extension $\mathbb{K}(\eta, d) \subseteq \mathbb{K}(\eta, \alpha)$. Since $1/t - d \in \mathbb{K}(\eta, d)(t)$, we know that

$$\frac{at+b}{t+d} \circ \left(\frac{1}{t} - d \right) = a + t(b - ad)$$

is also a linear fraction associated to $\mathcal{U}'$ (for the extension $\mathbb{K}(\eta, \gamma) \subseteq \mathbb{K}(\eta, \alpha)$ with primitive element α). In this case the denominator is 1, so $\mathcal{U}'$ must be a line.

To sum up, $\mathcal{U}'$, the witness variety of $\mathcal{C}$ for the extension $\mathbb{K}(\gamma) \subseteq \mathbb{K}(\alpha)$ with primitive element α is a line, defined over $\mathbb{K}(\gamma)$, so it has an associated unit of the form $f_1 t + f_2 \in \mathbb{K}(\alpha)(t)$ such that $\phi(f_1 t + f_2) \in \mathbb{K}(\gamma)(t)$.

For the second part, let η be a quadratic element in the conditions of Theorem 3.9 such that it does not belong to the normal closure of $\mathbb{L}(\alpha)$ over $\mathbb{K}$. Let $u = \frac{at+b}{t+d} \in \mathbb{K}(\eta, \alpha)(t)$ be a unit that reparametrizes $\mathcal{C}$ over $\mathbb{K}(\eta)$. Let $\phi_e = \phi(e_1 t + e_2) \in \mathbb{L}(t)$. On the one hand,

$$w_1(t) = \frac{\frac{a-e_2}{e_1} t + \frac{b - e_2 d}{e_1}}{t + d} = \left(\frac{t - e_2}{e_1} \right) \circ \frac{at+b}{t+d} \in \mathbb{L}(\eta, \alpha, e_1, e_2)(t)$$

reparametrizes ϕ_e over $\mathbb{K}(\eta)$. On the other hand, by Theorem 3.1, there is another unit $w_2 = \frac{a't+b'}{t+d'} \in \mathbb{L}(\eta)(t)$ that reparametrizes ϕ_e over $\mathbb{K}(\eta)$. Then, there is a unit $w_3 = \frac{a''t+b''}{t+d''} \in \mathbb{K}(\eta)(t)$ such that $w_1 = w_2 \circ w_3 \in \mathbb{L}(\eta)(t)$. Hence, $d \in \mathbb{L}(\eta)$. So

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L}(\eta) : \mathbb{K}(\eta)] = [\mathbb{K}(\eta, d) : \mathbb{K}(\eta)][\mathbb{L}(\eta) : \mathbb{K}(\eta, d)].$$

Since $[\mathbb{K}(\eta, d) : \mathbb{K}(\eta)] = r$, $[\mathbb{L} : \mathbb{K}] \geq r$ and we have the first item.

Now, $\mathbb{K}(\eta, d)$ is $\mathbb{K}(\eta)$-isomorphic to $\mathbb{K}(\eta, \gamma)$. Then $\mathbb{L}(\eta)$ contains a field that is $\mathbb{K}(\eta)$-isomorphic to $\mathbb{K}(\eta, \gamma)$. Let $M(x)$ be the minimal polynomial of γ over $\mathbb{K}$. Then, there is a root of $M(x)$ in $\mathbb{L}(\eta)$. By the election of η, this root belongs to $\mathbb{L}$. So $\mathbb{L}$ contains a field $\mathbb{K}$-isomorphic to $\mathbb{K}(\gamma)$. The rest of the items follows easily from this one and the proof of the first part. $\square$

As a corollary of this Theorem, we have the following algorithm to compute an optimal affine reparametrization.

Algorithm 4.4.
input: A computable field $\mathbb{K}$ (with factorization) finitely generated over $\mathbb{Q}$. An element α algebraic of degree n over $\mathbb{K}$. A birational parametrization $\phi(t) \in \mathbb{K}(t)^N$ of a rational curve $\mathcal{C}$.
output:

– If $\mathcal{C}$ is not defined over $\mathbb{K}$ return "FAIL".

– If $\mathcal{C}$ is defined over $\mathbb{K}$ return $at + b \in \mathbb{K}(\alpha)[t]$ such that

$$[\mathbb{K}(\text{coeffs}(\phi(at+b))) : \mathbb{K}]$$

is the smallest possible.

1. Compute the witness variety $\mathcal{Z}$ of $\mathcal{C}$ for the extension $[\mathbb{K}(\alpha) : \mathbb{K}]$ and primitive element α.

2. Compute the points at infinity of $\mathcal{Z}$.

3. If there are no points at infinity ($\mathcal{Z}$ is zero dimensional) then **Return** "FAIL".

4. Else, (there are finitely many points at infinity).
   Compute a point $[b_0 : \ldots : b_{n-1} : 0]$ at infinity with coefficients in $\mathbb{K}(\alpha)$.

5. Compute $r = [\mathbb{K}(b_0, \ldots, b_{n-1}) : \mathbb{K}]$.

6. If $r = [\mathbb{K}(\alpha) : \mathbb{K}]$, **Return** $at + b = t$.

7. If $r = 1$

   - Compute $(\psi_0, \ldots, \psi_{n-1})$ a linear parametrization of the unique one-dimensional component of $\mathcal{Z}$ over $\mathbb{K}$ (easy, since it is a line defined over $\mathbb{K}$).
   - **Return** $at + b = \sum_{i=0}^{n-1} \psi_i(t)\alpha^i$.

8. (Else) Compute the minimal polynomial of α over $\mathbb{K}(b_0, \ldots, b_{n-1})$.

9. Compute the witness variety $\mathcal{Z}'$ of $\mathcal{C}$ for the extension $\mathbb{K}(b_0, \ldots, b_{n-1}) \subseteq \mathbb{K}(\alpha)$.

10. Compute $(\psi_0, \ldots, \psi_{n/r-1})$ a linear parametrization of the unique one-dimensional component of $\mathcal{Z}'$ (which is a line) with coefficients in the field $\mathbb{K}(b_0, \ldots, b_{n-1})$.

11. **Return** $at + b = \sum_{i=0}^{n/r-1} \psi_i(t)\alpha^i$.

Example 4.5. *Let α be a root of $x^4 - 4x^3 + 12x^2 - 16x + 8$, and let $\mathcal{C}$ be the parametric curve given by*

$$x = \frac{-6 + 18\alpha - 9\alpha^2 + 6\alpha^3 + (44 - 52\alpha + 18\alpha^2 - 4\alpha^3)t - 4t^2}{-22 + 26\alpha - 9\alpha^2 + 2\alpha^3 + 4t},$$

$$y = \frac{-12 - 2\alpha + 9\alpha^2 - \alpha^3 + \left(4 + 4\alpha + 4\alpha^2\right)t + \left(12 - 16\alpha + 6\alpha^2 - 2\alpha^3\right)t^2}{-22 + 26\alpha - 9\alpha^2 + 2\alpha^3 + 4t}$$

The hypercircle $\mathcal{U}$ associated to this curve has implicit equations:

$$\{4t_2 + 12t_3 - 3, 5 + 2t_1 - 16t_3, 2t_0^2 + 24t_3t_0 + 80t_3^2 - 10t_0 - 52t_3 + 15\}.$$

One can easily check that this hypercircle is non primitive, because it is contained in the hyperplane $4t_2 + 12t_3 - 3$. Moreover, from its equations, it is a conic. The points at infinity are:

$$[2\gamma : 8 : -3 : 1 : 0]$$

where γ is a root of $x^2 + 6x + 10$. The roots of this polynomial in $\mathbb{Q}(\alpha)$ are $-4\alpha + 3/2\alpha^2 - 1/2\alpha^3$ and $-6 + 4\alpha - 3/2\alpha^2 + 1/2\alpha^3$. Choose for example $\gamma = -4\alpha + 3/2\alpha^2 - 1/2\alpha^3$. Then, the minimal polynomial of α over $\mathbb{Q}(\gamma)$ is $x^2 + (-8 - 2\gamma)x + 8 + 2\gamma$. Now, we rewrite the parametrization of $\mathcal{C}$ over this extension of fields:

$$x = \frac{(21 + 9\gamma)\alpha - 39 - 15\gamma + ((6\gamma + 14)\alpha - 2\gamma - 2)t - 2t^2}{1 + \gamma + (-3\gamma - 7)\alpha + 2t}$$

$$y = \frac{-30 - 5\gamma + (6\gamma + 27)\alpha + (-14 - 4\gamma + (18 + 4\gamma)\alpha)t + (2\gamma + 6)t^2}{1 + \gamma + (-3\gamma - 7)\alpha + 2t}$$

we compute the hypercircle associated to the extension $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\gamma, \alpha)$. We know that it will be a line, in fact, the computation yields $2t_1 - 3\gamma - 7$, that can be parametrized by $(s, (3\gamma + 7)/2)$. Hence, the affine substitution $t = t + (3\gamma + 7)/2\alpha$ in the parametrization yields a parametrization over the subfield $\mathbb{Q}(\gamma)$

$$x = \frac{-3\gamma - 2t^2\gamma + 4t\gamma - 5 + 6t^2 - 4t^3}{5 - 8t + 4t^2}$$

$$y = 2\frac{7t\gamma + 2t^3\gamma - 3\gamma - 6t^2\gamma - 10 + 23t + 6t^3 - 19t^2}{5 - 8t + 4t^2}$$

Acknowledgements

References

[1] Carlos Andradas, Tomás Recio, and J. Rafael Sendra. A relatively optimal rational space curve reparametrization algorithm through canonical divisors. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 349–355 (electronic), New York, 1997. ACM.

[2] Carlos Andradas, Tomás Recio, and J. Rafael Sendra. Base field restriction techniques for parametric curves. In *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC)*, pages 17–22 (electronic), New York, 1999. ACM.

[3] Carlos Andradas, Tomás Recio, J. Rafael Sendra, and Luis Felipe Tabera. On the simplification of the coefficients of a parametrization. *J. Symbolic Comput.*, To appear, 2008. doi:10.1016/j.jsc.2008.09.001.

[4] Claude Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable*. Mathematical Surveys, No. VI. American Mathematical Society, New York, N. Y., 1951.

[5] P. Gianni and B. Trager. Integral closure of Noetherian rings. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 212–216 (electronic), New York, 1997. ACM.

[6] D. Hilbert and A. Hurwitz. Über die diophantischen Gleichungen vom Geschlecht Null. *Acta Math.*, 14(1):217–224, 1890.

[7] Tomás Recio and J. Rafael Sendra. A really elementary proof of real Lüroth's theorem. *Rev. Mat. Univ. Complut. Madrid*, 10(Special Issue, suppl.):283–290, 1997. Real algebraic and analytic geometry (Segovia, 1995).

[8] Tomás Recio, J. Rafael Sendra, Luis Felipe Tabera, and Carlos Villarino. Generalizing circles over algebraic extensions. *Manuscript*, 2006.

[9] Tomás Recio, J. Rafael Sendra, and Carlos Villarino. From hypercircles to units. In *ISSAC 2004*, pages 258–265. ACM, New York, 2004.

[10] J. Rafael Sendra and Carlos Villarino. Optimal reparametrization of polynomial algebraic curves. *Internat. J. Comput. Geom. Appl.*, 11(4):439–453, 2001.

[11] J. Rafael Sendra and Carlos Villarino. Algebraically optimal parametrizations of quasi-polynomial algebraic curves. *J. Algebra Appl.*, 1(1):51–74, 2002.

[12] J. Rafael Sendra and Franz Winkler. Parametrization of algebraic curves over optimal field extensions. *J. Symbolic Comput.*, 23(2-3):191–207, 1997. Parametric algebraic curves and applications (Albuquerque, NM, 1995).

[13] Luis Felipe Tabera. *Two Tools in Algebraic Geometry: Construction of Configurations in Tropical Geometry and Hypercircles for the Simplification of Parametric Curves*. PhD thesis, Universidad de Cantabria, Université de Rennes I, 2007.

[14] Oscar Zariski and Pierre Samuel. *Commutative algebra. Vol. II*. Springer-Verlag, New York, 1975. Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.

Luis Felipe Tabera
IMDEA Mathematics Foundation
Módulo C-IX 3th floor Facultad de Ciencias - UAM
Ciudad Universitaria de Cantoblanco
E-28049 Madrid, Spain.
e-mail: luis.tabera@imdea.org
http://personales.unican.es/taberalf/